2021 June

George Kaloudis

The Investor's Perspective on the Bitcoin Taproot Upgrade

Content

INTRODUCTION

To many investors, bitcoin represents a new and exciting aspirational store of value. Bitcoin's potential to become a store of value has earned it the label, "gold 2.0" and "digital gold."

In a handful of ways, Bitcoin is an upgrade from gold as a store of value. For example, bitcoin's scarcity is provable and the cost of storing immense value in bitcoin is a small fraction of gold's. Gold, on the other hand, has a five-millennia head start on bitcoin and boasts far lower volatility. Plus, gold has industrial use cases and is in demand for its perceived beauty.

Where bitcoin and gold diverge entirely is the fact that the Bitcoin network is an upgradable technology. Gold in a vault will remain gold. There is no chance gold will turn into lead, silver or some improved version of gold. In contrast, the Bitcoin network can change.

Bitcoin is an upgradable technology that can adapt over time as user, miner and developer needs change. On June 12, 2021, enough Bitcoin miners signaled support for a technological upgrade known as the Taproot Upgrade (Taproot). Taproot is a bundle of three upgrades that are aimed at improving network security, privacy and scalability. Taproot is the most significant upgrade to the Bitcoin network since the activation of the block capacity enhancement of Segregated Witness in 2017.

The expected benefits of the upgrades include:

- Consolidation of all types of bitcoin transaction outputs into a singular Taproot output that will improve privacy by making different types of transactions indistinguishable.
- Improved Bitcoin programmability (i.e., so-called "smart contracts").
- Enhanced data efficiency by using a more efficient signature algorithm and transaction structuring method.
- Boosted security due to the addition of a new signature scheme, making it a dual-signature blockchain.

It does not come without its risks, which include:

- Low adoption rate shows that Bitcoin users are not interested in using Bitcoin for anything new.
- Low adoption rate negates potential privacy benefits.
- New signature scheme may prove less "quantum resistant" than the current scheme.
- Potential for fracturing in the Bitcoin community due to disagreement over the Taproot upgrade - similar to the controversy over Segregated Witness that led to Bitcoin Cash.

We will expand upon these benefits and risks in the report in order to provide a backdrop for Bitcoin as a technology investment. In addition, we will discuss how upgrades have historically been implemented on the Bitcoin network.

Throughout, we capitalize the blockchain (Bitcoin, Ethereum) and use lowercase or trading symbols (bitcoin/BTC, ether/ETH) for the asset. Dollars are U.S. dollars ($USD): Nothing in this report should be considered investment advice.

THE TAPROOT UPGRADE

The Taproot Upgrade consists of three separate Bitcoin Improvement Proposals (BIPs), 340, 341 and 342.

In short, **Taproot is designed to improve Bitcoin's security, privacy and efficiency**.

Taproot would achieve these improvements through:

- **MASTs** change the way spending conditions are structured by reducing required inputs, which decreases each transaction's data footprint.
- **Pay-to-Taproot** produces a single "Taproot" output on the Bitcoin network, regardless of transaction type, improving transaction privacy and efficiency.
- **Schnorr signatures** replaces the current cryptographic signature scheme, known as ECDSA (Elliptic Curve Digital Signature Algorithm).

These three BIPs are being implemented together in order to encourage wallets and service providers to update their software just once in order to maximize the adoption of the full suite, thus improving Bitcoin for as many users as possible.

Benefits of Taproot

Taproot will expand the usability and total addressable market of Bitcoin. Quantifying that increase is difficult, but the qualitative benefits are as follows:

Richer Application Development

Bitcoin is usually not associated with smart contracts, which are self-executing digital contracts with the terms and execution written as code or scripts. Instead, the Ethereum blockchain is typically associated with smart contracts and the development of blockchain-based applications that use them.

However, Bitcoin does have native smart contract capabilities. Bitcoin transactions can be programmed to time payments when certain constraints are met or missed. Bitcoin smart contracts are currently used for multi-signature wallets, to enable the Lightning Network (Lightning or LN) and to "lock" units of bitcoin, ensuring they will remain unspent for a period of time.

As it stands now, creating these particular Bitcoin contracts is cumbersome and expensive. Additionally, if a user wanted to send a complex Bitcoin transaction, they would have to put the

script inside each transaction input. When those scripts are then executed, all the conditions, including the ones that were not met, will be revealed. As such, transactions involving Bitcoin contracts are data-heavy and bad for privacy. Taproot will make on-chain smart contracts more viable by breaking up the execution of the Bitcoin scripts so that only the script that is executed is revealed.

Taproot also improves the usability of what are known as Discreet Log Contracts (DLCs) which can be used to construct Bitcoin smart contracts. Somewhat notoriously, two Bitcoin company founders, Nicolas Dorier of BTCPay Server and Chris Stewart of Suredbits, entered into a DLC in 2020 to bet on the result of the United States presidential election. With Taproot, DLCs will have a smaller on-chain footprint, which encourages smart contracting on Bitcoin.

All said, the smart contracts touted as flexible and revolutionary by many are currently too difficult to achieve on Bitcoin to be commonplace. So, although Taproot will make Bitcoin smart contracts more viable, we will not see a rise of Bitcoin decentralized applications (dapps) and decentralized autonomous organizations (DAOs) that characterize the Ethereum blockchain in the near term. Instead, we would more likely see a rise of simple Bitcoin smart contracts in insurance payouts, residential real estate transactions or financial annuity products, which represent meaningful growth opportunities, such as:

- Life insurance payouts could be programmed upon satisfactory receipt of a death certificate or some equivalent - 2019 payouts in the U.S. exceeded $760BN.
- Residential real estate transactions can trigger final settlement when a seller's bank confirmed receipt of payment for the balance of the mortgage - 5.8 million residential real estate units were sold in the U.S. the seasonally adjusted annual period May 2021 for a median price of ~$350,000.
- Financial annuities could pay out programmatically over a specified period of time - U.S. annuity assets in 2020 exceeded $3TN.

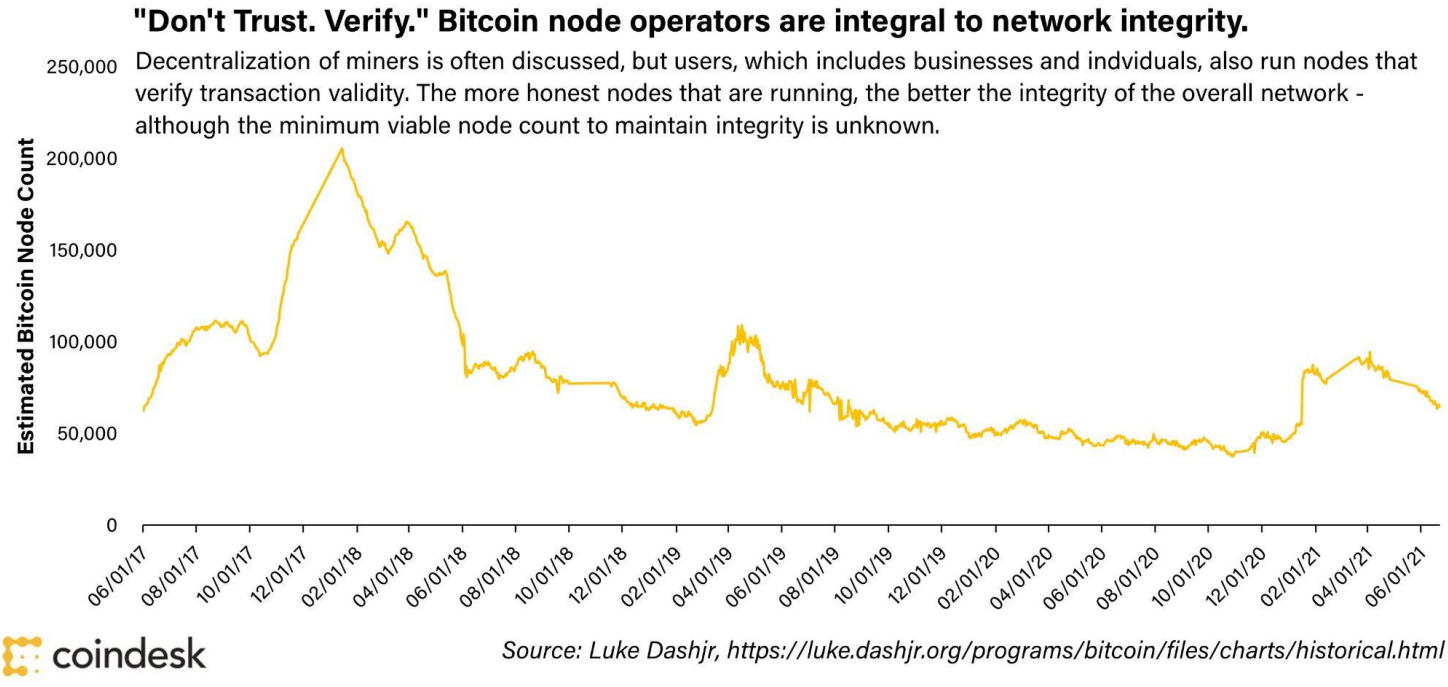
Bitcoin's path to penetration into these markets is unclear. The most visible factor may be customer demand for all or a portion of proceeds to be paid in bitcoin.

Lastly, the insurance companies that issue life insurance and sell annuity products represent some of the most conservative risk profiles in the financial world, given they were established in the mid-1800s with "existence into perpetuity" in mind. If these companies are to succumb to whatever demand there is from their customers for a foray into the digital asset and blockchain market, it will more likely come in the form of something Bitcoin-related. Compared to Ethereum, Bitcoin is the more conservative, predictable blockchain from a technological perspective (see "**Activation of Upgrades**" section below). It is also more gold- and money-like than any of its competitors, so a grasp of its value proposition is more obvious. Not to mention, insurer MassMutual has already invested in Bitcoin and Bitcoin companies.

Data Efficiency

Schnorr signatures will improve the efficiency of single-signer transactions. Schnorr signatures are 64 bytes (unit of digital information) while ECDSA signatures are 71 - 73 bytes, which should result in a ~11% efficiency gain per transaction. There is no guarantee that Taproot-enabled transactions will be adopted by the network: users will remain free to stick with Bitcoin's legacy transaction technology. However, if Taproot transactions are adopted, fewer resources will be demanded to run one of the full nodes that validate transactions and maintain the network. This encourages users to run their own full nodes, which improves Bitcoin's decentralization. Bitcoin's decentralization allows it to be permissionless and censorship-resistant, two critical characteristics to its value proposition. A deterioration in decentralization would weaken Bitcoin and could greatly hurt its value.

A dropping node count might not be a problem for the network, provided that enough nodes are still operating. That amount is not really knowable, but in reality the number itself is unimportant. What does matter is that users who meaningfully transact on the Bitcoin network are checking transactions against their own node and there are enough nodes to service chain downloads for new nodes. This is similar to the Bitcoin network's mining hashrate, where more hashrate is "better," but less hashrate is not necessarily any "worse," until it reaches a certain, unknown threshold.



Source: Luke Dashjr, https://luke.dashjr.org/programs/bitcoin/files/charts/historical.html

Figure 1

Additionally, since Schnorr signatures are a less data-heavy signature scheme, Taproot may increase the average number of transactions that can be included per block. This could in turn lead to lower transaction fees for users.

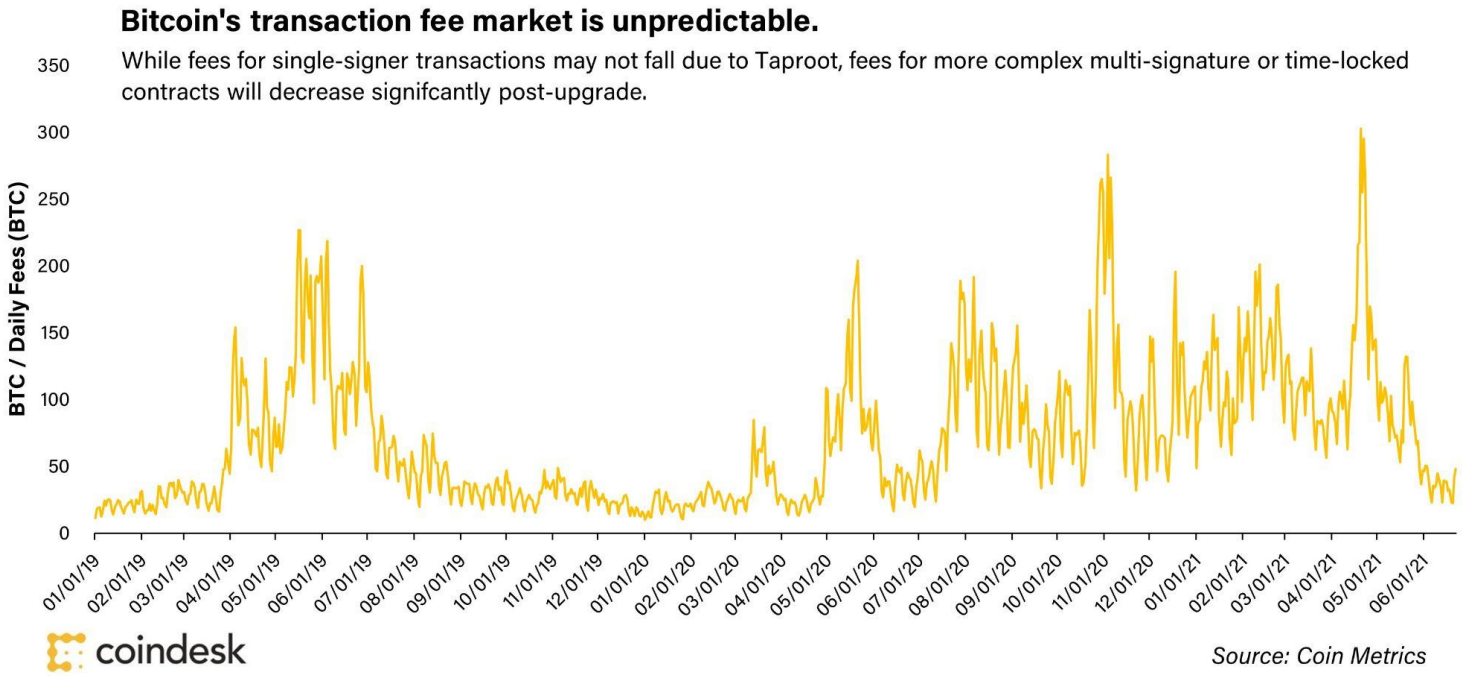


Figure 2

However, transaction fees swing wildly (see **Fig. 2**), depending on a whole litany of influences. We can say though that when it comes to more complex multi-signature or time-locked transactions, it is almost certain that those particular fees will decrease significantly with Taproot.

Improved Wallet Functionality, Usability and Privacy

Taproot is designed to improve multi-signature wallet functionality. Multi-signature wallets are wallets that require more than one signer to unlock funds, which makes them more secure than single-signature wallets. Taproot is designed to make these transactions more data-efficient. There is also a privacy upgrade at play here. Taproot transactions will mask the spending conditions of multi-signature wallets. Currently, multi-signature wallets on Bitcoin are constructed using smart contracts. As discussed above, Bitcoin smart contracts currently reveal all spending conditions, every time a transaction takes place.

As an example, a multi-signature wallet's revealed conditions could specify that transactions must be signed by three of five valid signatures or by one master signature. Even if the master signature is never used, the blockchain would reveal the public address connected to the master signature with every transaction, posing a potential security threat.

Taproot patches that up in two ways:

1. Potential spending conditions of the funds will not be revealed whenever funds are moved.
2. Since Pay-to-Taproot makes all transaction outputs look the same, no one can tell if the company is using multi-signature or not.

While privacy improves with Taproot, it does not make Bitcoin blockchain forensics impossible. Bitcoin will remain a pseudonymous network with a publicly auditable digital paper trail. Bitcoin will not become a privacy coin, like Monero or Zcash, with Taproot and it will remain less private than cash.

The chart below (**Fig. 3**) shows the amount of bitcoin held in multi-signature wallets since 2018. It has grown ~55% since 2018, but has remained stagnant since an all-time high in July 2019. The lack of growth the last two years can give us pause. Should Taproot be widely adopted we may see a boost in adoption of multi-signature solutions by privacy-minded individuals and companies. On the other hand, the slow-to-no growth in multi-signature wallet balances in recent years indicates demand for this feature may be lacking. It is also worth mentioning that with Taproot this type of analysis will not be possible going forward since transaction outputs will all look the same.

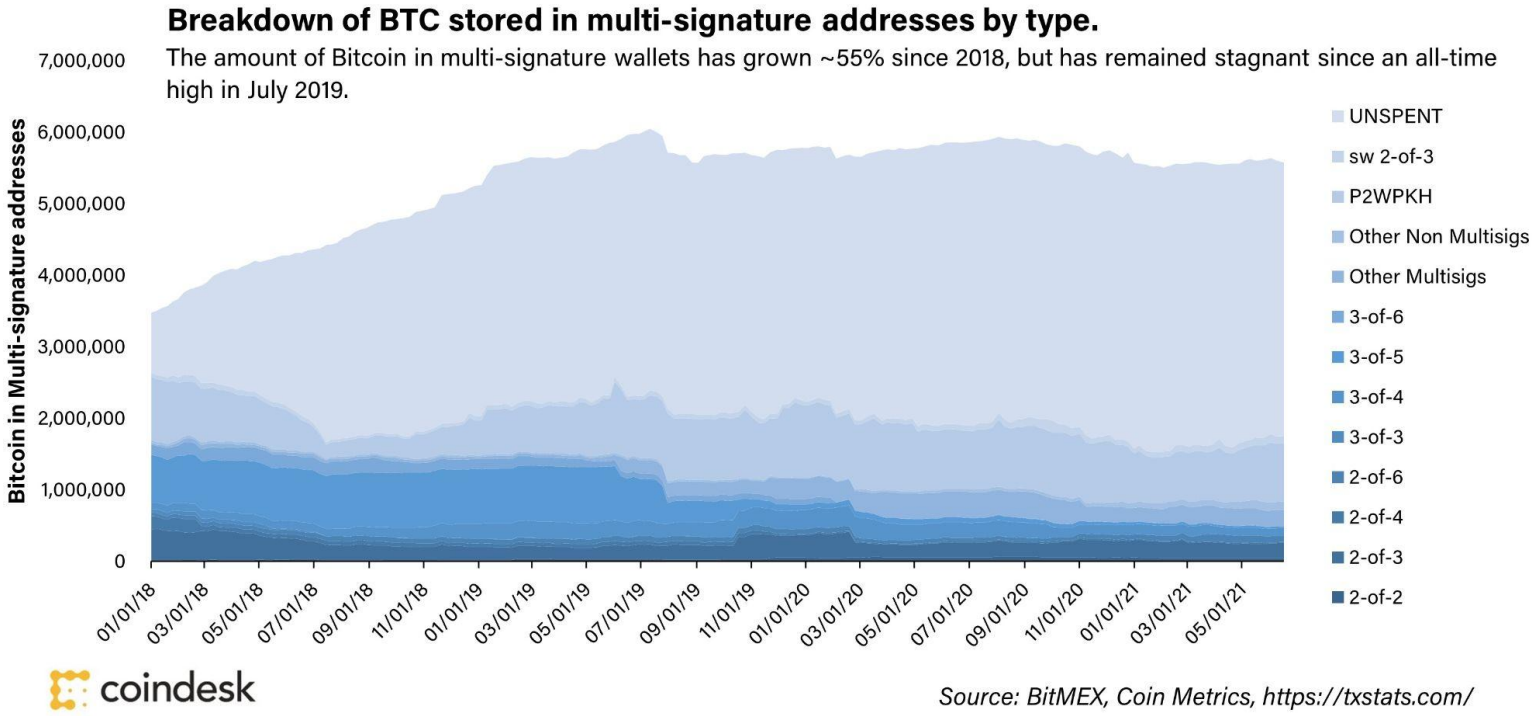


Figure 3

Lastly, Taproot will enable the use and construction of wallet solutions and signature schemes that build on top of a Schnorr signature characteristic known as "linearity," which means signatures can be consolidated. One such example is that it would now be practical to create a multi-signature wallet that degrades over time by requiring three signatures, but then only requiring two, if the funds remain untouched for a certain period of time.

Advancement of Second Layer Scaling Solutions

Taproot allows for improvements to layer-2 networks such as the Lightning Network, which sit on top of Bitcoin. Taproot will upgrade Lightning Network capabilities by replacing Hash Time Locked Contracts (HTLCs) with Point Time Locked Contracts (PTLCs). Lightning Network is a

commerce-oriented service that allows parties to transact in bitcoin more rapidly and cheaply. Using PTLCs means payments will be routed using regular public keys, providing privacy features similar to those designed for multi-signature wallets. PTLCs can also enable blockchain escrow conditions and improve the use of oracles to prompt the facilitation of payments.

The Lightning Network has grown unevenly since its launch in 2018. Taproot could accelerate adoption. From an investment perspective, increased transactability of Bitcoin is positive since an improvement to any particular use case will expand its total addressable market and growth prospects.

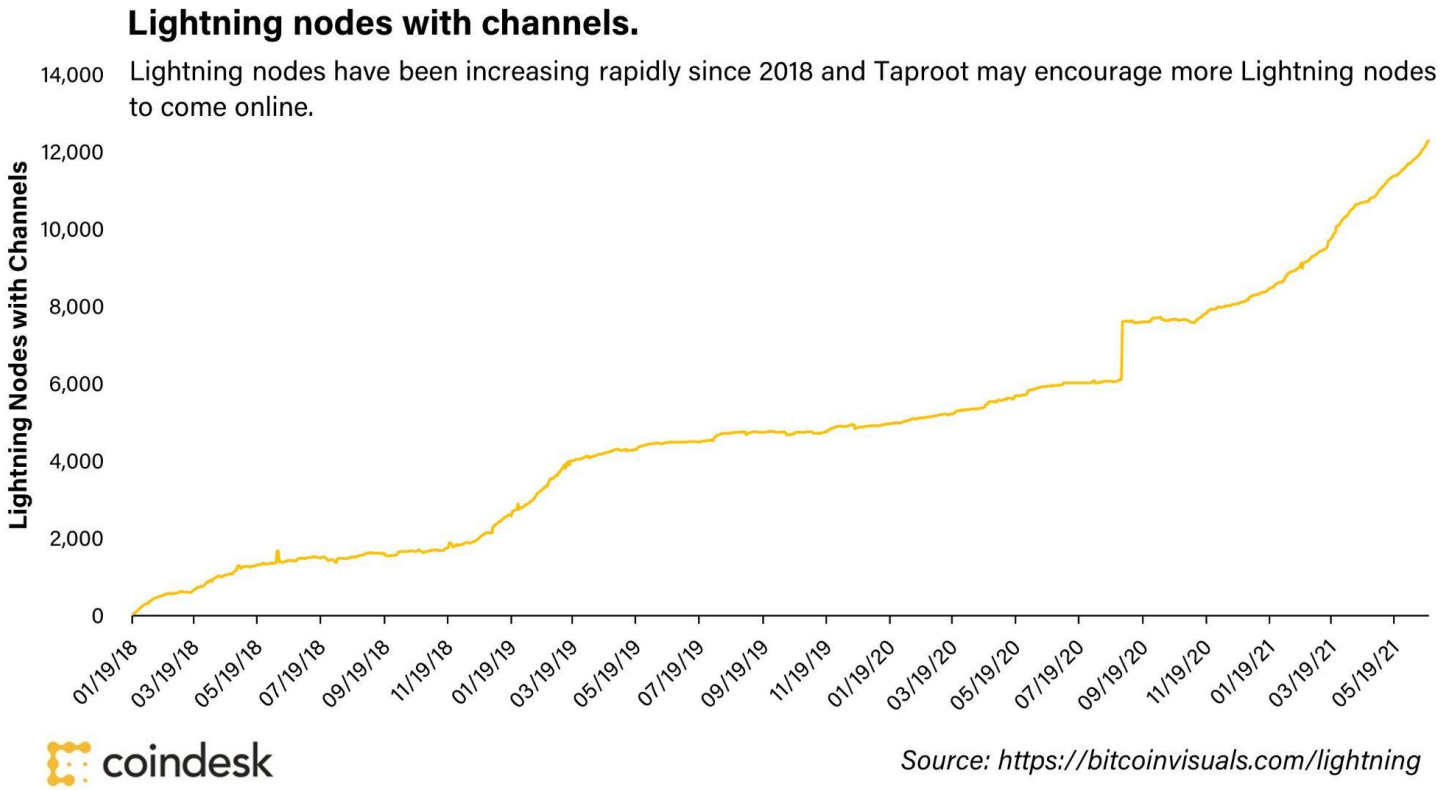


Figure 4

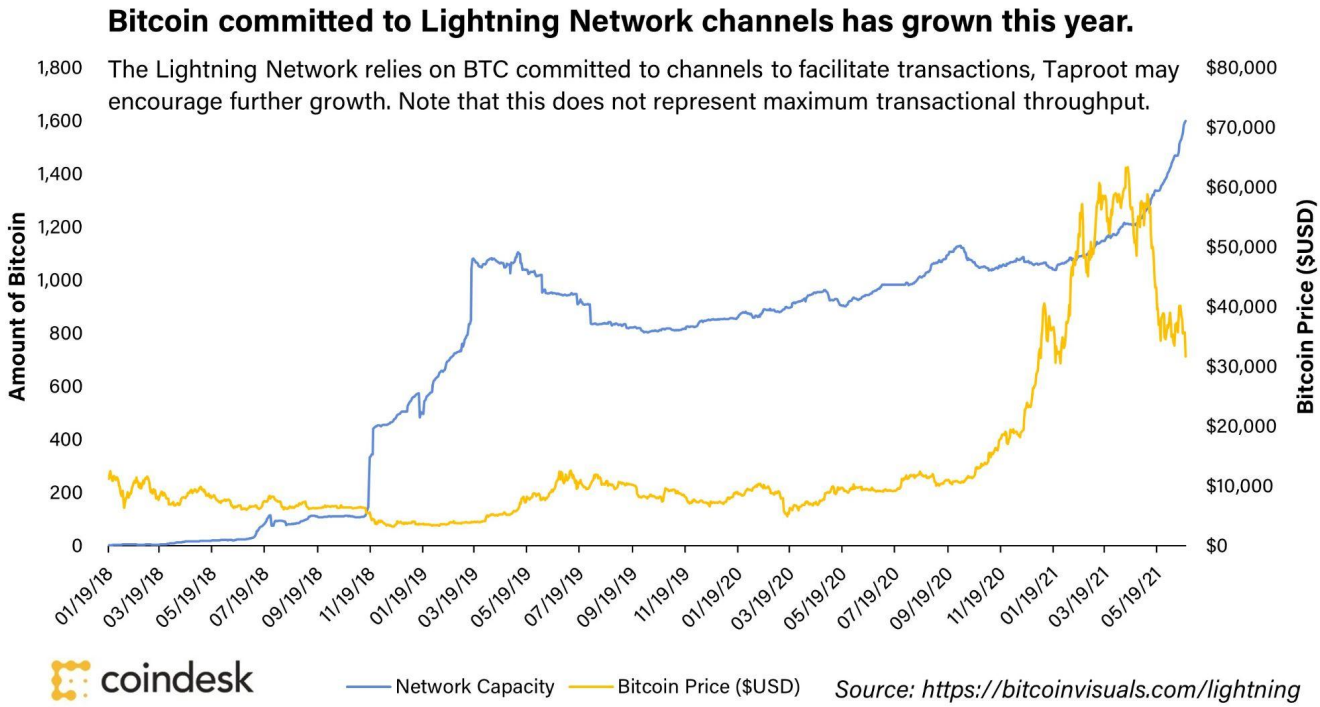


Figure 5

Tailwinds for Lightning Network include El Salvador's acceptance of Bitcoin (enshrining Lightning as a Bitcoin commerce service), as well as funding and partnership announcements by Lightning-enabled payments services, such as Strike, Fold and Moon.

These tailwinds, coupled with the improvements from Taproot should bode well for Bitcoin as an investment. The growth of layer-2 payments services has the potential to help establish another core use narrative for bitcoin. Bitcoin has emerged as a gold-like digital asset, but its potential as a peer-to-peer digital currency is mostly unrealized, as yet.

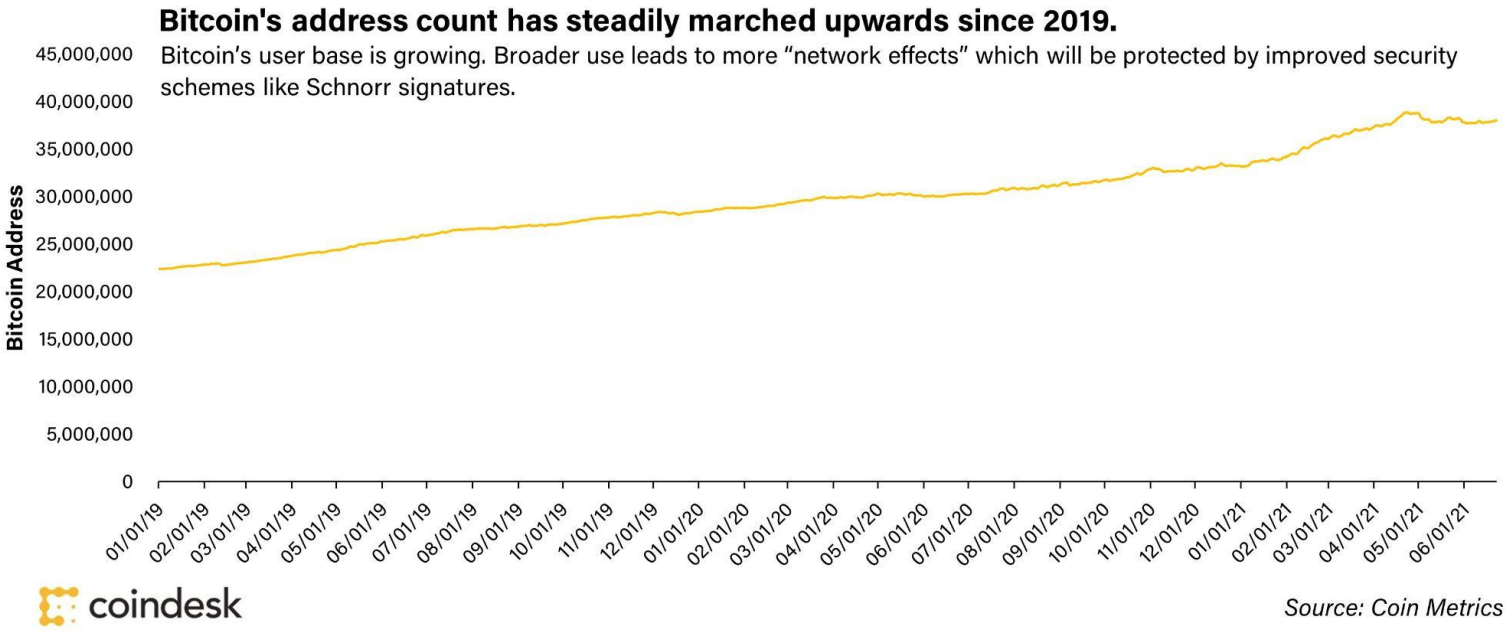


Figure 6

Potential Drawbacks and Threats Related to the Taproot Upgrade

Low Adoption Rate

The biggest threat related to Taproot is the potential that only a small number of users and service providers adopt and implement the upgrade.

- Low adoption rates of a highly anticipated upgrade could indicate that most users are not interested in using Bitcoin for anything new. For new uses, Bitcoin users may prefer a different cryptocurrency or service.
- Users shunning an upgrade that makes Bitcoin more flexible diminishes Bitcoin's growth prospects as it closes the door on potential upgrades down the road.
- Some of Taproot's privacy features only work in a crowd: if few users adopt Taproot transactions, it's easy to pinpoint those addresses as belonging to entities requiring multi-signature security.
- A rejection of Taproot would highlight a weakness in the Bitcoin community if an update supported by developers and vocal users falls flat.

What could lukewarm acceptance of Taproot mean for the future of Bitcoin? Would Bitcoin succumb to its digital gold narrative as its primary value proposition? Maybe, and if so, there is potential that Bitcoin will never become a reliable platform for peer-to-peer digital cash or software development. That would not necessarily preclude Bitcoin achieving its potential as "digital gold."

Quantum Resistance

Schnorr signatures may also prove to be less "quantum resistant" than ECDSA. Quantum resistance refers to the Bitcoin protocol's ability to withstand an attack from quantum computers. While quantum computers are not known to be a threat now, they may emerge as a threat in the future. However, with Taproot, Bitcoin will have two signature types securing the network. If Schnorr signatures are not quantum resistant, then users can utilize ECDSA. If ECDSA is not appropriate, the protocol can add other signature schemes that are quantum resistant.

Bitcoin Community Fracturing

A benefit of a technology that depends on consensus to bring about change is that any perceived drawback will be amplified and can lead to rejection of a new idea. Herein lies another potential drawback to Taproot. If Taproot activation turns contentious, then there may be a fracturing in the Bitcoin network with a part of the community deciding that they will no longer use Bitcoin.

ACTIVATION OF UPGRADES

Although the details of Taproot itself are paramount to investors, it is also important to cover the way upgrades to Bitcoin are typically proposed and implemented to get a full picture of the current situation.

Since Bitcoin is open source, anyone can propose improvements. The improvement process was formalized early in Bitcoin's history through a process called Bitcoin Improvement Proposals (BIPs). While the finer details of the BIP process are not crucial to understand deeply since they are highly technical, we should note that BIPs are generally uncommon, especially when compared to other protocols, and BIPs are typically small tweaks as opposed to extensive upgrades.

Bitcoin Moves Slowly

Since Bitcoin's inception in 2009, there have been a total of 145 BIPs submitted, an average of ~12 per year. By way of comparison, the second largest digital asset network by market value, Ethereum, has had 342 EIPs (Ethereum Improvement Proposals) submitted since its inception in 2015, an average of ~58 per year. Bitcoin moves slower than other cryptocurrencies, from a technological standpoint.

The Bitcoin development and user community have stressed that reliability and uptime is one of the more important aspects of Bitcoin. Of the 145 submitted BIPs, only 46 (~30%) have been implemented into the protocol. Not to mention, eight of these (~6%) are Informational BIPs, which simply describe a design issue, or provide general guidelines or information to the Bitcoin community, but do not propose a new feature. In general, BIPs have been implemented as soft forks, which means that the upgrade will remain backwards compatible with out-of-date versions of Bitcoin software. By contrast, Ethereum has had multiple hard forks, which force all users to upgrade.

CONCLUSION

Beyond improving Bitcoin, Taproot is a reminder that Bitcoin is a technology. It has the potential to change as required, in order to improve usability and user experience. Inspired entrepreneurs will continue to develop their own versions of Bitcoin killers. If Taproot is successful, it will demonstrate that Bitcoin can adapt.

With the reminder that Bitcoin is a technology, we should add that Bitcoin is a unique technology investment for the following reasons:

Bitcoin is Liquid

Venture capital and growth equity investments into technology companies are illiquid, especially when compared to Bitcoin. As a reference point, in 1Q2021 U.S. Private Equity Exit Value was ~$162BN while Bitcoin exchange volume was ~$405BN.

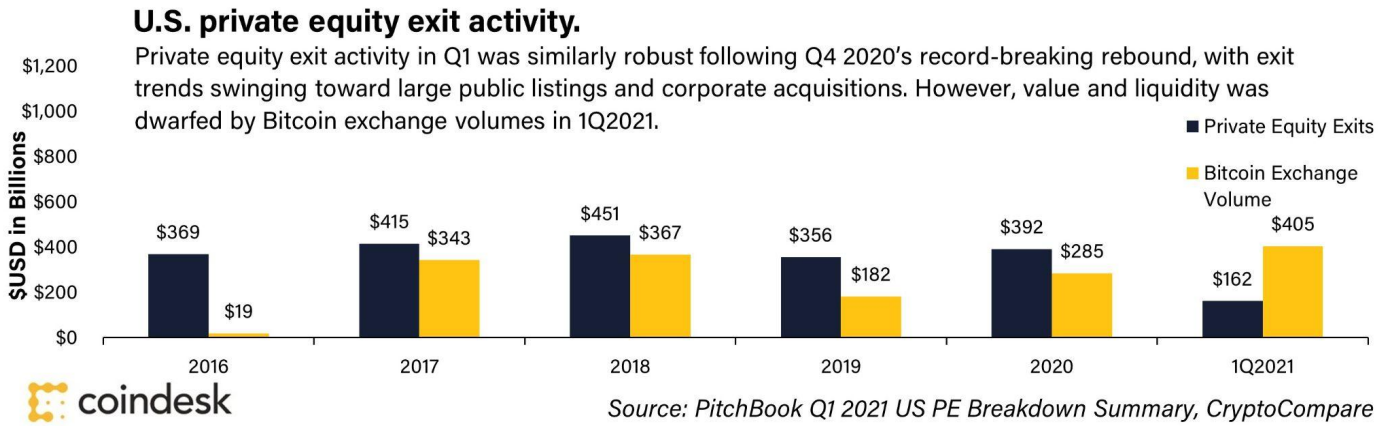


Figure 7

Bitcoin is Transparent

Bitcoin provides complete transparency in what upgrades are being implemented, proposed and rejected. An enterprising investor could go in and self-audit progress, code and conversation around BIPs. If an investor does not like the code or the direction Bitcoin is heading, they can make their opinion known and directly propose changes. There is no other investment that provides that level of transparency into day-to-day guts of the operation.

Bitcoin's Total Addressable Market (TAM)

Investors view TAM as a proxy for an investment's underlying growth potential, so long as it can be captured. Bitcoin's TAM is staggering, depending on if you view Bitcoin as a technology for payment settlement, store of value or global reserve currency. At its largest, Bitcoin's TAM outsizes any other technology investment, even when compared against the largest publics.

As bitcoin approaches one of the largest technology upgrades in its history to date, investors assessing the risks and benefits it implies for bitcoin as a technology investment must keep in mind these unique characteristics.

CoinDesk Research offers reports and multimedia programming by independent experts on crypto industry trends and assets, to help professional investors make sense of the rapidly evolving concepts and data.

You can see more of our work, as well as a wide range of reports from some of the industry's top research teams, in our **Research Hub** at **www.coindesk.com/research**.

Be sure to follow us on Twitter at **@coindeskdata**.

You can reach us at **research@coindesk.com**.

CoinDesk Research is: **Galen Moore**, **Christine Kim**, **Shuai Hao** and **George Kaloudis**.